Information-technology Promotion Agency, Japan

JPCERT CC®

プレスリリース
2012 年 7 月 23 日
独立行政法人情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター

ソフトウェア等の脆弱性関連情報に関する届出状況 [2012 年第 2 四半期（4 月～6 月）]

～ ウェブサイトの管理に利用される CMS もしくは CMS プラグインの脆弱（ぜいじゃく）性に注意 ～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）およびJPCERT/CC（一般社団法人JPCERTコーディネーションセンター、代表理事：歌代 和正）は、2012 年第 2 四半期（4 月～6 月）の脆弱性関連情報の届出状況 (*1) をまとめました。

（1）脆弱性の届出件数の累計が 7,752 件に（別紙 1　1.参照）

2012 年第 2 四半期の IPA への脆弱性関連情報の届出件数は 169 件で、内訳はソフトウェア製品に関するものが 45 件、ウェブサイト（ウェブアプリケーション）に関するものが 124 件でした。これにより、2004 年 7 月の届出受付開始からの累計は、ソフトウェア製品に関するものが 1,383 件、ウェブサイトに関するものが 6,369 件、合計 7,752 件となりました。

（2）脆弱性の修正完了件数の累計が 4,900 件を超過（別紙 1　2.参照）

ソフトウェア製品の脆弱性の届出のうち、JPCERT/CCが調整を行い、製品開発者が修正を完了し、2012 年第 2 四半期にJVN (*2) で対策情報を公表したものは 33 件（累計 639 件）でした。また、ウェブサイトの脆弱性の届出のうち、IPAがウェブサイト運営者に通知し、2012 年第 2 四半期に修正を完了したものは 192 件（累計 4,265 件）でした。これにより、ソフトウェア製品を含めた脆弱性の修正件数は累計で 4,904 件となりました。

（3）CMS もしくは CMS プラグインの脆弱性（別紙 1　3.参照）

2012 年第 2 四半期に受理し取扱したソフトウェア製品の脆弱性の届出において、届出件数（42 件のうち 9 件）および公表件数（33 件のうち 7 件）のそれぞれ 21%がCMS[3]もしくはCMSプラグインの脆弱性でした。

ウェブサイトの管理に利用されている CMS もしくは CMS のプラグインの脆弱性が悪用されると、ウェブサイトの内容が改ざんまたは、任意のプログラムが実行されるなどの被害が発生する可能性があります。

ウェブサイト運営者は、ウェブサイトにおいて利用されているソフトウェア製品の脆弱性対策情報を緊密に収集し、適切な脆弱性対策（バージョンアップ等）の実施が必要です。

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 渡辺／大森
Tel: 03-5978-7527　Fax: 03-5978-7518
E-mail: vuln-inq@ipa.go.jp
JPCERT/CC 情報流通対策グループ　古田
Tel: 03-3518-4600　Fax: 03-3518-4602
E-mail: office@jpcert.or.jp

■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／佐々木
Tel: 03-5978-7503　Fax: 03-5978-7510
E-mail: pr-inq@ipa.go.jp
JPCERT/CC 事業推進基盤グループ 広報 江田
Tel: 03-3518-4600　Fax: 03-3518-4602
E-mail: pr@jpcert.or.jp

(*1) ソフトウェア等脆弱性関連情報取扱基準：経済産業省告示（http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf）に基づき、2004 年 7 月より開始しました。IPA は届出受付・分析、JPCERT/CC は国内の製品開発者などの関連組織との調整を行っています。

(*2) Japan Vulnerability Notes：脆弱性対策情報ポータルサイト。国内で利用されている製品の脆弱性対策情報を公表し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。http://jvn.jp/

(*3) Content Management System：ウェブサイトのコンテンツ（テキストや画像など）を統合的に管理するためのウェブアプリケーションソフト。

別紙 1

2012 年第 2 四半期　ソフトウェア等の脆弱性関連情報に関する届出状況（総括）

1.脆弱性関連情報の届出状況

～ 脆弱性の届出件数の累計が 7,752 件になりました ～

表 1.　届出件数

分類	今期件数	累計件数
ソフトウェア製品	**45** 件	**1,383** 件
ウェブサイト	**124** 件	**6,369** 件
合計	**169** 件	**7,752** 件

表 1 は 2012 年第 2 四半期の IPA への脆弱性関連情報の届出件数および届出受付開始（2004 年 7 月 8 日）から今四半期までの累計件数を示しています。今期の届出件数はソフトウェア製品に関するもの 45 件、ウェブサイト（ウェブアプリケーション）に関するもの 124 件、合計 169 件でした。届出受付開始からの累計件数は、ソフトウェア製品に関するもの 1,383 件、ウェブサイトに関するもの 6,369 件、合計 7,752 件となりました。ウェブサイトに関する届出が全体の 82%を占めています。

図 1 のグラフは過去 3 年間の届出件数の四半期別推移を示したものです。今四半期のソフトウェア製品の届出は前四半期と比較して微減となり、ウェブサイトに関する届出は前四半期の約 6 割となっています。表 2 は過去 3 年間の四半期別の累計届出件数および 1 就業日あたりの届出件数の推移です。1 就業日あたりの届出件数は 2012 年第 2 四半期末で 3.99 (*1) 件となりました。

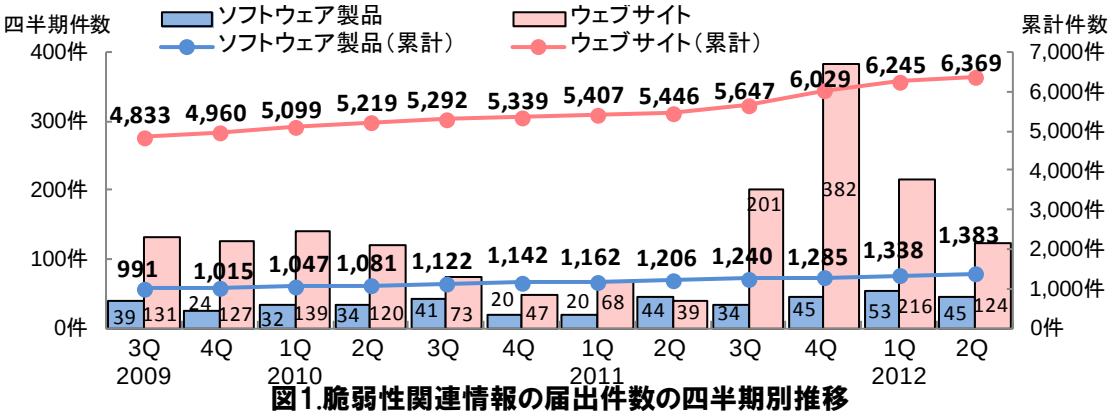


図1.脆弱性関連情報の届出件数の四半期別推移

表 2. 届出件数（過去 3 年間）

	2009 3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q
累計届出件数[件]	5,824	5,975	6,146	6,300	6,414	6,481	6,569	6,652	6,887	7,314	7,583	7,752
1就業日あたり[件/日]	4.56	4.47	4.40	4.32	4.22	4.10	4.01	3.92	3.91	4.02	4.03	3.99

図 2 のグラフは今四半期に届出されたソフトウェア製品の届出 45 件のうち、不受理とした届出を除いた 42 件の製品種類の内訳を、図 3 はソフトウェア製品の脅威 (*2) の内訳を示したものです。製品種類で分類すると「ウェブアプリケーションソフト (*3) 」が最も多く、次いで「ルータ」と「グループウェア」となっています。脅威で分類すると「任意のスクリプトの実行」が最も多く、これに「サービス不能」、そして「なりすまし」が次いでいます。

(*1) 1 就業日あたりの届出件数は、「累計届出件数」/「届出受付開始からの就業日数」にて算出
(*2) ソフトウェア製品の脆弱性が悪用された場合に生じる脅威
(*3) ウェブサーバ側で動作し、サービスを提供するソフトウェア（ブログ、掲示板等）

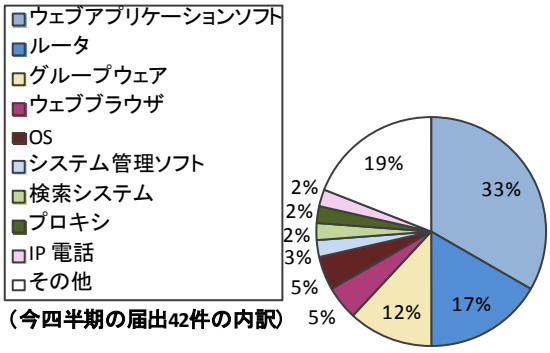


図2. 今四半期のソフトウェア製品種類の内訳

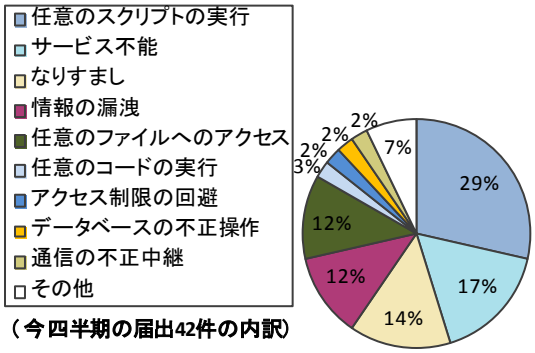


図3. 今四半期のソフトウェア製品の脅威の内訳

図 4 のグラフは今四半期に届出されたウェブサイトの届出 124 件のうち、不受理とした届出を除いた 123 件のウェブサイト運営主体の内訳を、図 5 は脆弱性の種類の内訳を示したものです。運営主体は「企業」が全体の 71%を占めています。また、脆弱性の種類は前四半期と同様に「クロスサイト・スクリプティング」が最も多く、全体の 87%を占めています。

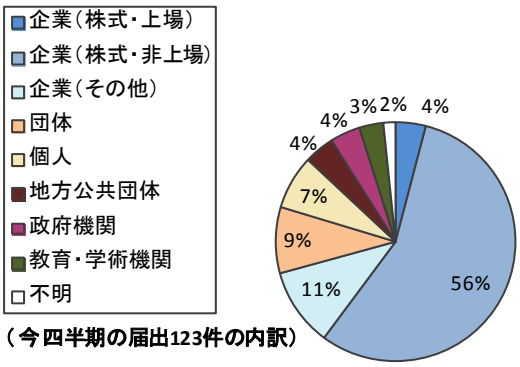


図4. 今四半期のウェブサイト運営主体の内訳

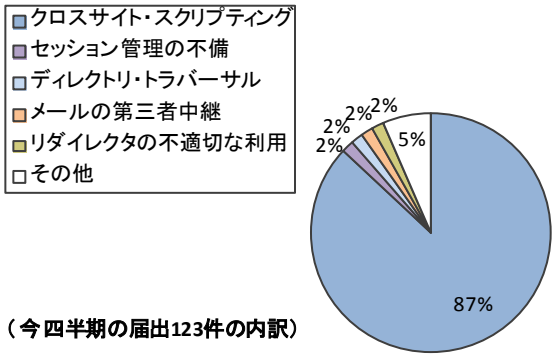


図5. 今四半期の脆弱性の種類の内訳

2.脆弱性の修正完了状況

～ ソフトウェア製品およびウェブサイトの修正件数が 4,900 件を超過しました ～

表 3 は 2012 年第 2 四半期のソフトウェア製品とウェブサイトの修正完了件数および届出受付開始から今四半期までの累計件数を示しています。

ソフトウェア製品の脆弱性の届出のうち、JPCERT/CCが調整を行い、製品開発者が修正を完了し、2012 年第 2 四半期にJVNで対策情報を公表したものは 33 件 (*4)（累計 639 件）でした。2010 年第 4 四半期以降は修正完了件数が 30 件前後で推移しています。

表 3.　修正完了件数

分類	今期件数	累計件数
ソフトウェア製品	**33** 件	**639** 件
ウェブサイト	**192** 件	**4,265** 件
合計	**225** 件	**4,904** 件

今四半期に対策情報を公表した 33 件のうち、届出を受理してから公表までに 45 日以上経過した届出は 23 件でした。**IPA および JPCERT/CC は、届出された脆弱性への対策および、製品利用者に対する脆弱性対策情報の公表への協力を引き続き製品開発者に期待します。**

ウェブサイトの脆弱性関連情報の届出のうち、IPA がウェブサイト運営者に通知を行い、 2012 年第 2 四半期に修正を完了したものは 192 件（累計 4,265 件）でした。修正を完了した 192 件の

(*4)　別紙 2 表 1-3 参照

対策内容の内訳は、ウェブアプリケーションを修正したものが 173 件（90%）、当該ページを削除したものが 19 件（10%）でした。なお、修正を完了した 192 件のうち 67 件（35%）は、届出から修正完了まで 90 日以上経過していました。**IPA はウェブサイト運営者による、速やかな対策実施を期待します。**

3. ソフトウェア製品の脆弱性関連情報に関する届出の傾向

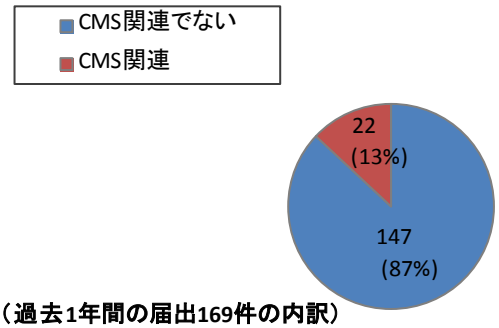
～ CMS もしくは CMS のプラグインにおける脆弱性 ～

2012 年は、CMS[5]やCMSのプラグインの脆弱性を悪用した攻撃による被害が確認されています。

過去 1 年間に受理したソフトウェア製品の届出において、CMS もしくは CMS プラグインにおける脆弱性の届出は 169 件のうち 22 件(13%)であり、全届出に占める割合は少ない状況です（図 6）。

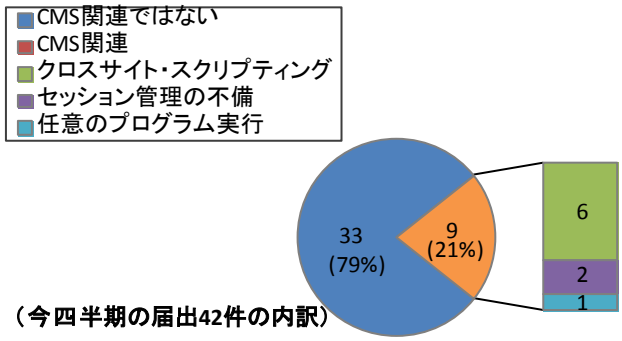
今四半期に受理したソフトウェア製品の届出 42 件においては、9 件（21%）がCMSもしくはCMSのプラグインにおける脆弱性の届出となり、全届出に占める割合が多くなっています。9 件の脆弱性の種類は「クロスサイト・スクリプティング」が 6 件、「セッション管理の不備」が 2 件、「任意のプログラム実行」が 1 件です（図 7）。また、今四半期に脆弱性が修正され対策情報をJVNで公表した 33 件のうち、7 件[6]（21%）がCMSもしくはCMSのプラグインでした。

ウェブサイトの管理に利用されている CMS もしくは CMS のプラグインの脆弱性が悪用されると、ウェブサイトの内容が改ざんまたは、任意のプログラムが実行されるなどの被害が発生する可能性があります。



（過去1年間の届出169件の内訳）

図6.過去1年間におけるCMSもしくはCMSのプラグインに関する届出



（今四半期の届出42件の内訳）

図7.今四半期におけるCMSもしくはCMSのプラグインに関する届出

ウェブサイト運営者は、ウェブサイトにおいて利用しているソフトウェア製品の脆弱性対策情報の緊密な収集と[7]、脆弱性対策（バージョンアップ等）の実施が必要です。

4. ウェブサイトの脆弱性関連情報に関する届出の傾向

～ ウェブサイトの脆弱性対策は速やかに実施を ～

届出受付開始（2004 年 7 月 8 日）から今四半期までに修正が完了したウェブサイトの届出のうち、90 日以内に修正が完了した割合は 66%でした。全届出の約半数を占めるクロスサイト・スクリプティングに関する届出のうち、2010 年以降の届出について、修正までに要した日数は、2010

(*5) Content Management System：ウェブサイトのコンテンツ（テキストや画像など）を統合的に管理するためのウェブアプリケーションソフト。

(*6) 別紙 2 表 1-3 の項番 2、4、12、13、18、20、25 が該当。

(*7) 届脆弱性対策情報の修正およびバージョンの確認の一助として、下記をご活用ください。
脆弱性対策情報データベース「JVN iPedia」：http://jvndb.jvn.jp/index.html
MyJVN 脆弱性対策情報収集ツール：http://jvndb.jvn.jp/apis/myjvn/mjcheck.html
MyJVN バージョンチェッカ（サーバ用）：http://jvndb.jvn.jp/apis/myjvn/vccheckserv.html。

年は 67%、2011 年は 64%、2012 年（6 月末時点）は 52%と、90 日以内に修正が完了する割合が低下しています（図 8）。これは、2012 年以降に届出されたウェブサイトを運営している組織の大半が、小規模の組織または個人が運営しているウェブサイトであるため、脆弱性対策に手が回らない状況であると推察されます。

ウェブサイトにクロスサイト・スクリプティングの脆弱性が存在する事によって、ウェブサイトの内容が改ざんされるなどの可能性があります。ウェブサイトの内容が改ざんされた結果、ウェブサイト利用者が偽のページに誘導されるなどによりフィッシング詐欺にあうなどの可能性があります。ウェブサイト利用者が被害を受けることにより、脆弱性があるウェブサイトを運営している組織自体の信用が毀損される場合があります。今四半期においてもウェブサイトの脆弱性を悪用してウェブサイトが改ざんされるという被害が発生していますので、組織として、速やかな脆弱性対策の実施が重要です。

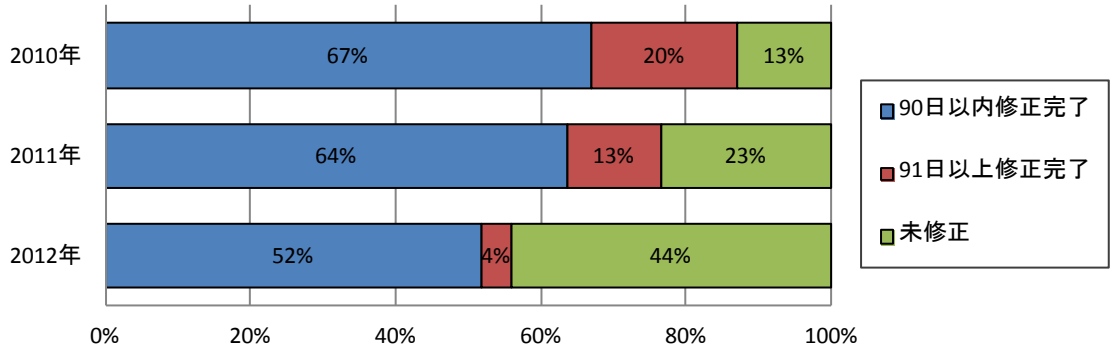


図8. 修正までに要した日数の割合（年別）

ウェブサイト運営者においては、脆弱性によって引き起こされる組織への影響を、技術者だけではなく、経営層も含め組織全体で認識し、脆弱性への対策は予算等の確保も含め計画的に講じることが重要です。また、届出された脆弱性について、届出された箇所以外にも同様な脆弱性が無いかの確認および、他の脆弱性がないか、全体的な見直しが実施されることを期待します。

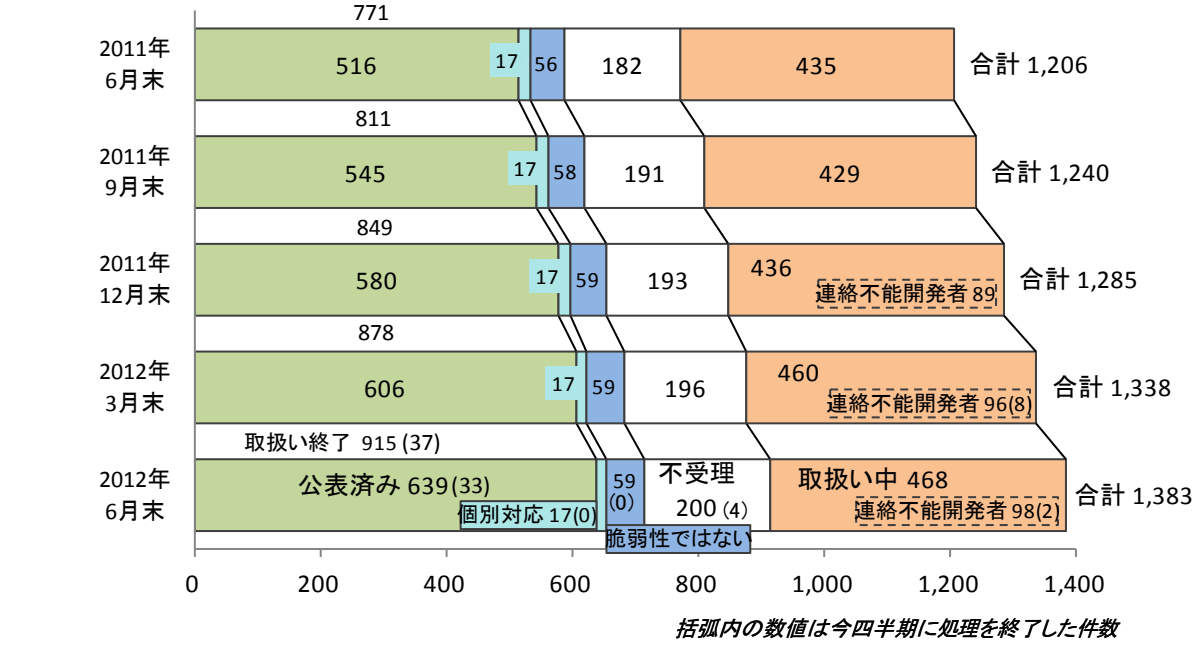
別紙 2

ソフトウェア等の脆弱性に関する届出の処理状況（詳細）

1. ソフトウェア製品の脆弱性の処理状況の詳細

1.1 ソフトウェア製品の脆弱性の処理状況

図 1-1 のグラフはソフトウェア製品の脆弱性関連情報の届出における、処理状況の推移を示したものです。今四半期に公表した脆弱性は 33 件（累計 639 件）です。また、製品開発者が「個別対応」したものは 0 件（累計 17 件）、製品開発者が「脆弱性ではない」と判断したものは 0 件（累計 59 件）、「不受理」としたものは 4 件 (*1)（累計 200 件）、取扱い中は 468 件です。取扱中の届出のうち 2 件について、連絡不能開発者 (*2) として連絡不能開発者一覧 (*3) にて公表しました。2012 年 6 月末時点の連絡不能開発者公表数は 98 件になります。



	公表済み	：JVN で脆弱性への対応状況を公表したもの
	個別対応	：製品開発者からの届出のうち、製品開発者が個別対応したもの
	脆弱性ではない	：製品開発者により脆弱性ではないと判断されたもの
	不受理	：告示で定める届出の対象に該当しないもの
	取扱い中	：製品開発者が調査、対応中のもの
	連絡不能開発者	：連絡不能開発者一覧にて公表したもの

図 1-1.ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

1.2 届出のあったソフトウェア製品の種類

届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品の脆弱性関連情報 1,383 件のうち、不受理とした届出を除いた 1,183 件について、図 1-2 のグラフは製品種類別の届出件数の割合を、図 1-3 は過去 2 年間の製品種類別の届出件数の四半期別推移をそれぞれ示したものです。

今四半期における製品種類は、「ウェブアプリケーション」が減少し、「グループウェア」と「ルータ」が増加しています。

(*1) 今四半期の届出の中で不受理とした 3 件、前四半期までの届出の中で今四半期に不受理とした 1 件です。
(*2) 届出を受け付けたソフトウェア製品の製品開発者に対して、一定期間にわたり連絡を試みても連絡が取れない場合、その製品開発者を「連絡不能開発者」と位置づけます。
(*3) 連絡不能開発者一覧：http://jvn.jp/reply/index.html

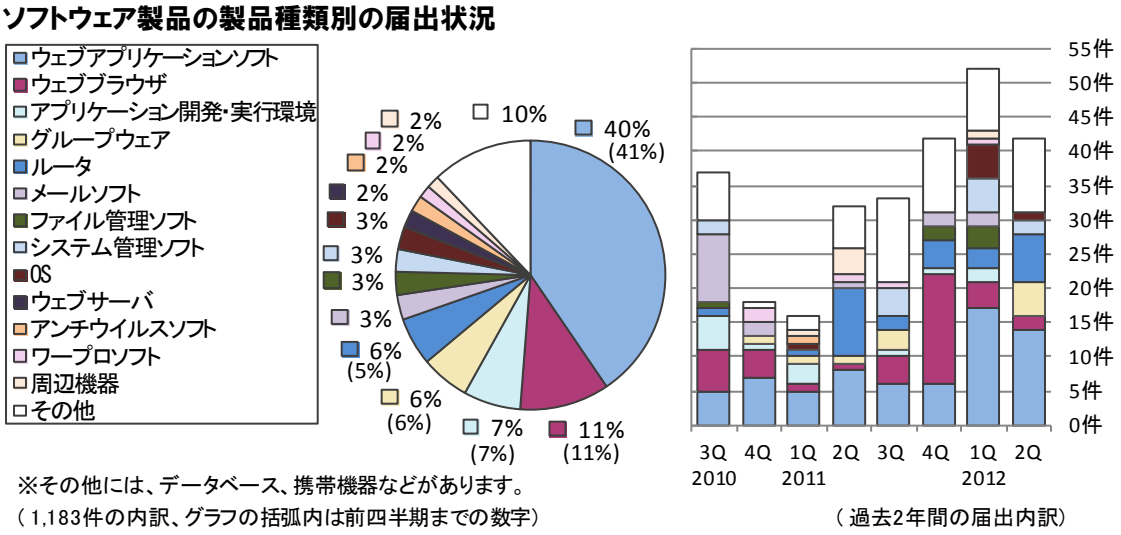


図1-2. 製品種類別の届出件数の割合　**図1-3. 製品種類別の届出件数（四半期別推移）**

届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品の脆弱性関連情報 1,383 件のうち、不受理とした届出を除いた 1,183 件について、図 1-4 のグラフはオープンソースソフトウェアとそれ以外のソフトウェアの脆弱性の届出件数の割合を、図 1-5 は過去 2 年間のオープンソースソフトウェアとそれ以外ソフトウェアの届出件数の四半期別推移をそれぞれ示したものです。届出受付開始から今四半期までの届出のうち、オープンソースソフトウェアの届出は約 33%となっています。また、今四半期はオープンソースソフトウェアとそれ以外のソフトウェアの届出が共に減少しています。

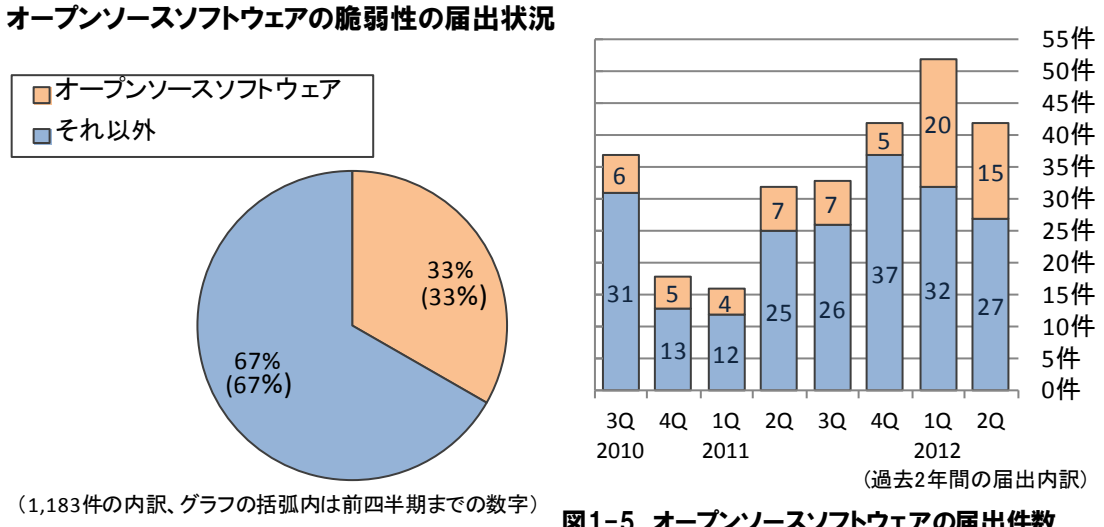


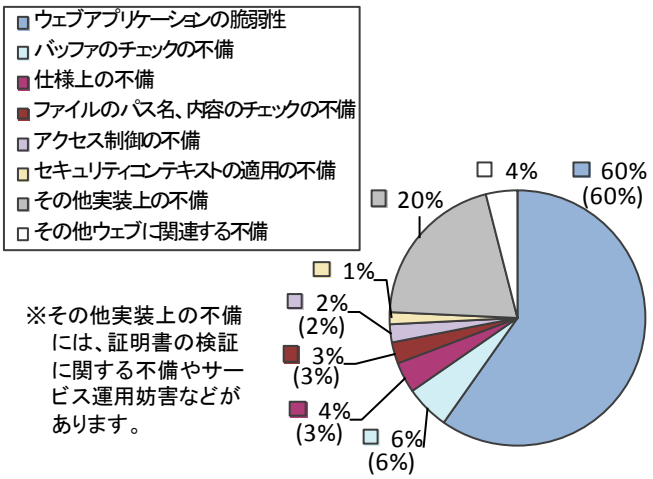
図1-4. オープンソースソフトウェアの届出件数の割合　**図1-5. オープンソースソフトウェアの届出件数（四半期別推移）**

1.3 脆弱性の原因と脅威

届出受付開始から今四半期までにIPAに届出のあったソフトウェア製品に関する脆弱性関連情報 1,383 件のうち、不受理とした届出を除いた 1,183 件について、図 1-6 のグラフは原因別(*4)の届出件数の割合を、図 1-7 のグラフは過去 2 年間の原因別届出件数の四半期別推移をそれぞれ示したものです。今四半期におけるソフトウェア製品の脆弱性の原因は、前四半期と同様に「ウェブアプリケーションの脆弱性」が最多となっています。

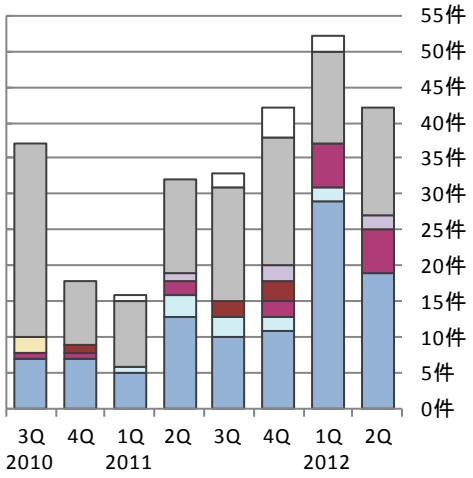
(*4)　それぞれの詳しい脆弱性の原因の説明については付表 1 を参照してください。

ソフトウェア製品の脆弱性の原因別の届出状況



（1,183件の内訳、グラフの括弧内は前四半期までの数字）

図1-6. 脆弱性の原因別の届出件数の割合

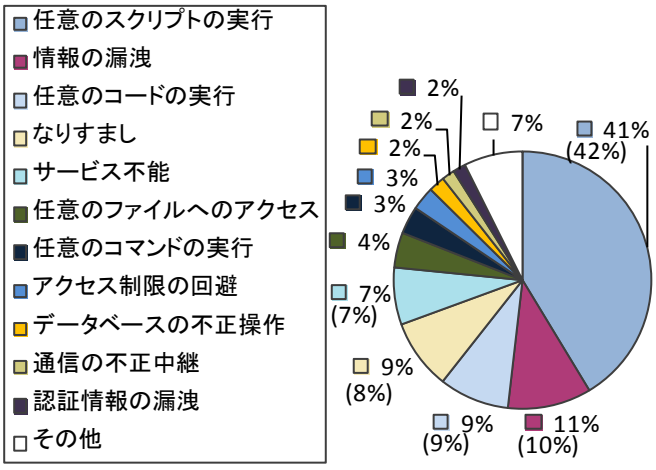


（過去2年間の届出内訳）

図1-7. 脆弱性の原因別の届出件数（四半期別推移）

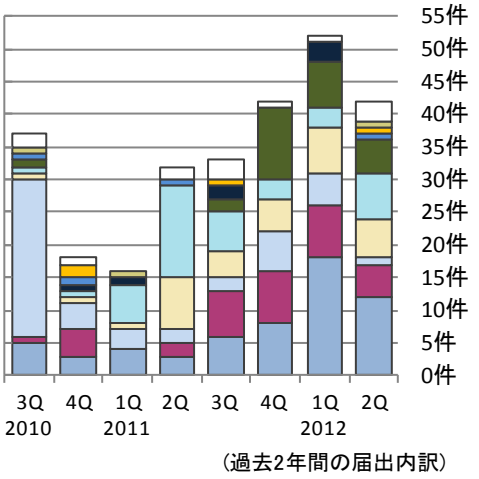
届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品に関する脆弱性関連情報 1,383 件のうち、不受理とした届出を除いた 1,183 件について、図 1-8 のグラフは脅威別の届出件数の割合を、図 1-9 は過去 2 年間の脅威別届出件数の四半期別推移をそれぞれ示したものです。「任意のスクリプトの実行」が届出受付開始から今四半期までの届出のうち約 4 割を占めています。また、今四半期は「任意のスクリプトの実行」が減少し、「サービス不能」が前四半期と比較して約 2 倍に増加しています。

ソフトウェア製品の脆弱性がもたらす脅威別の届出状況



（1,183件の内訳、グラフの括弧内は前四半期までの数字）

図1-8. 脆弱性がもたらす脅威別の届出件数の割合



（過去2年間の届出内訳）

図1-9. 脆弱性がもたらす脅威別の届出件数（四半期別推移）

1.4 ソフトウェア製品の脆弱性情報の調整および公表状況

表 1-1 は今四半期の脆弱性の公表件数および届出受付開始から今四半期までの累計公表件数を示しています。JPCERT/CCは、2 種類の脆弱性関連情報について、日本国内の製品開発者や関係者との調整、および海外CSIRTの協力のもと海外の製品開発者との調整を行っています[*5]。これらの脆弱性関連情報に対する製品開発者の対応状況は、IPAとJPCERT/CCが共同運営している脆弱性対策情報ポータルサイトJVN（Japan Vulnerability Notes）（URL： http://jvn.jp/ ）において公表しています。図 1-10 のグラフは、届出受付開始から今四半期までの届出の中で、対策情報を公表した 1,430 件について、過去 3 年間の公表件数の四半期別推移を示したものです。

[*5] JPCERT/CC 活動概要 Page16~22（https://www.jpcert.or.jp/pr/2012/PR20120712.pdf）を参照下さい。

表 1-1. 脆弱性関連情報の提供元別 脆弱性公表件数

	情報提供元	今期件数	累計件数
①	国内外の発見者から IPA に届出があったもの、および、製品開発者自身から自社製品の脆弱性、対策方法について届出を受けたもの	33 件	639 件
②	海外 CSIRT 等と連携して公表したもの	36 件	791 件
	合計	69 件	1,430 件

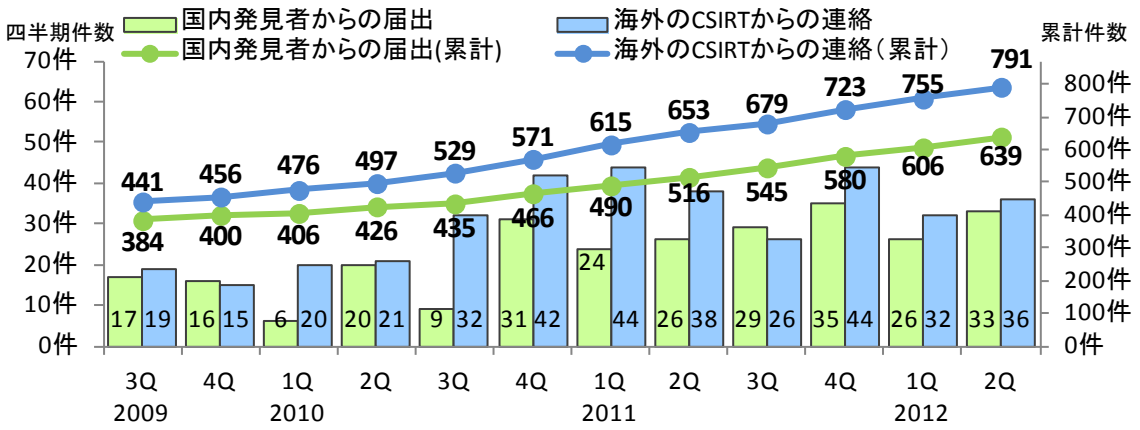


図1−10. ソフトウェア製品の脆弱性対策情報の公表件数

（1）国内外の発見者および製品開発者から届出があり、公表した脆弱性

届出受付開始から今四半期までに届出のあったソフトウェア製品の脆弱性関連情報（表 1-1 の①）について、図 1-11 は受理してから JVN 公表するまでに要した日数を示したものです。表 1-2 は過去 3 年間における 45 日以内に公表した件数の割合推移を四半期別に示したものです。45 日以内に公表した件数は 2012 年第 2 四半期で 34%、45 日を超過した件数は 66%です。製品開発者は脆弱性を攻撃された場合の危険性を認識し、迅速な対策を講じる必要があります。

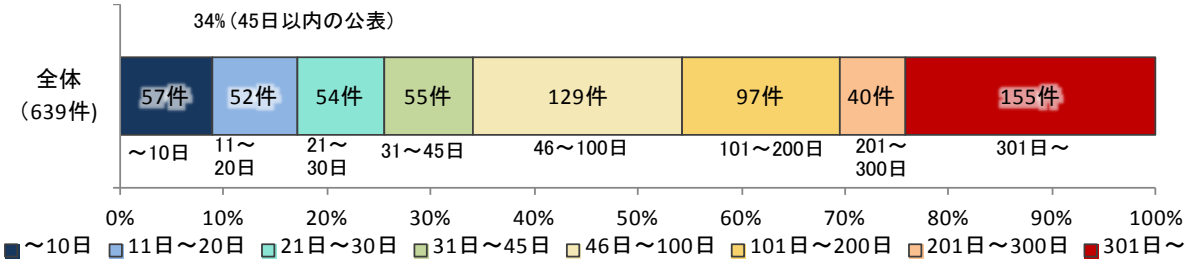


図1−11. ソフトウェア製品の脆弱性公表日数

表 1-2. 45 日以内に公表した件数の割合推移（四半期別）

2009 3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q
35%	35%	35%	36%	36%	38%	38%	36%	34%	33%	34%	34%

表 1-3 は国内の発見者および製品開発者から届出があり、今四半期に JVN 公表した脆弱性を示しています。オープンソースソフトウェアに関し公表したものが 11 件（表 1-3 の*1）、製品開発者自身から届けられた自社製品の脆弱性が 4 件（表 1-3 の*2）、組込みソフトウェア製品の脆弱性が 3 件（表 1-3 の*3）ありました。

表 1-3. 2012 年第 2 四半期に JVN で公表した脆弱性

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0～10.0				
1 (*3)	「LAN-W300N/R」シリーズにおけるアクセス制限不備の脆弱性	無線 LAN ルータ「LAN-W300N/R」シリーズには、アクセス制限不備の脆弱性がありました。このため、第三者によりウェブ管理画面にアクセスされてしまう可能性がありました。	2012 年 5 月 25 日	7.5
2 (*1)	「Segue」における SQL インジェクションの脆弱性	ショッピングサイト構築ソフト「Segue」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。	2012 年 6 月 1 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
3 (*2) (*3)	東芝テック製「e-Studio」シリーズにおける認証回避の脆弱性	複合機「e-Studio」には、認証回避の脆弱性がありました。このため、第三者によりウェブ管理画面にアクセスされる可能性がありました。	2012 年 4 月 5 日	6.4
4 (*1)	「せん茶 SNS」におけるセッション固定の脆弱性	SNS 構築ソフト「せん茶 SNS」には、セッション ID を正しく処理できない問題がありました。このため、第三者により正規のユーザになりすまされる可能性がありました。	2012 年 4 月 5 日	5.8
5 (*1)	「ActiveScriptRuby」に HTML 上で任意の Ruby スクリプトを実行可能な脆弱性	Ruby 実行ソフト「ActiveScriptRuby」には、ウェブブラウザで HTML を表示した際に、任意の Ruby スクリプトが実行可能な脆弱性がありました。このため、第三者により情報を取得されたり、サービス運用妨害 (DoS) 攻撃を受けたりする可能性がありました。	2012 年 4 月 13 日	5.8
6	「どこでもリクナビ 2013」におけるクロスサイト・スクリプティングの脆弱性	Google Chrome の拡張機能「どこでもリクナビ 2013」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 4 月 13 日	5.8
7	複数のジャストシステム製品における DLL 読み込みに関する脆弱性	複数のジャストシステム製品には、DLL を読み込む際の DLL 検索パスに問題があり、意図しない DLL を読み込んでしまう脆弱性がありました。このため、第三者によりプログラムを実行している権限で任意のコードを実行される可能性がありました。	2012 年 4 月 24 日	6.8
8 (*2)	複数のジャストシステム製品におけるバッファオーバーフローの脆弱性	複数のジャストシステム製品には、画像ファイルの処理にバッファオーバーフローの脆弱性がありました。このため、第三者により任意のコードを実行される可能性がありました。	2012 年 4 月 24 日	6.8
9	「sp モードメールアプリ」における SSL サーバ証明書の検証不備の脆弱性	Android アプリケーション「sp モードメールアプリ」には、SSL サーバ証明書の検証を適切に処理しない問題がありました。このため、第三者によって通信内容を傍受される可能性がありました。	2012 年 4 月 26 日	4.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
10 (*1)	「OSQA」におけるクロスサイト・スクリプティングの脆弱性	コンテンツ管理システム「OSQA」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 4 月 26 日	4.3
11	KENT-WEB 製「WEB MART」におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築システム「WEB MART」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 5 月 15 日	4.3
12 (*1) (*2)	「baserCMS」におけるセッション管理不備の脆弱性	コンテンツ管理システム「baserCMS」には、セッション管理不備の脆弱性がありました。このため、第三者により管理者権限でログインされる可能性がありました。	2012 年 5 月 15 日	4.0
13 (*1)	「Drupal」の Form API における送信先 URL を検証しない脆弱性	コンテンツ管理システム「Drupal」には、送信先 の URL を検証しない脆弱性の存在がありました。このため、第三者により認証情報などを窃取される可能性がありました。	2012 年 5 月 17 日	4.3
14 (*1)	「RSSOwl」において任意のスクリプトが実行される脆弱性	RSS/Atom フィードリーダー「RSSOwl」には、任意のスクリプトが実行される脆弱性がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 5 月 25 日	4.3
15	Sybase 製「EAServer」におけるクロスサイト・スクリプティングの脆弱性	アプリケーションサーバ「EAServer」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 5 月 25 日	4.3
16	「Opera」における SSL サーバ証明書の検証不備の脆弱性	ウェブブラウザ「Opera」には、SSL サーバ証明書の検証を適切に処理しない問題がありました。このため、不正な SSL サーバ証明書を使用しているサーバに接続しても警告が出ず、フィッシングなどの被害にあう可能性がありました。	2012 年 5 月 25 日	4.3
17 (*1)	「Roundcube Webmail」において任意のスクリプトが実行される脆弱性	ウェブメールソフト「Roundcube Webmail」には、任意のスクリプトが実行される脆弱性がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 5 月 25 日	4.3
18	「Segue」におけるクロスサイト・スクリプティングの脆弱性	コンテンツ管理システム「Segue」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 1 日	4.3
19	「@WEB ショッピングカート」におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築ソフト「@WEB ショッピングカート」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 5 日	4.3
20 (*1)	WordPress 用プラグイン「WassUp」におけるクロスサイト・スクリプティングの脆弱性	WordPress 用プラグイン「WassUp」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 6 日	5.0
21 (*2) (*3)	「SEIL」シリーズにおけるアクセス制限不備の脆弱性	ルータ製品「SEIL」シリーズには、アクセス制限不備の脆弱性がありました。このため、HTTP プロキシに接続可能な第三者によって、URL フィルタ等の制限を回避される可能性がありました。	2012 年 6 月 6 日	5.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
22	「FeedDemon」において任意のスクリプトが実行される脆弱性	RSS/Atom フィードリーダー「FeedDemon」には、任意のスクリプトが実行される脆弱性がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 7 日	4.3
23	「WEB PATIO」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「WEB PATIO」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 19 日	4.3
24	「SmallPICT」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「SmallPICT」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 19 日	4.3
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
25 (*1)	「せん茶 SNS」におけるクロスサイト・リクエスト・フォージェリの脆弱性	SNS 構築ソフト「せん茶 SNS」には、クロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、当該製品にログインした状態で悪意あるページを読み込んだ場合、意図しない投稿をされる可能性がありました。	2012 年 4 月 5 日	2.6
26	「TwitRocker2 (Android 版)」における WebView クラスに関する脆弱性	Android アプリケーション「TwitRocker2 (Android 版)」には、WebView クラスに関する問題がありました。このため、第三者により当該製品のデータ領域にある情報が窃取される可能性がありました。	2012 年 4 月 20 日	2.6
27	KENT-WEB 製「WEB MART」におけるクロスサイト・スクリプティングの脆弱性	ショッピングサイト構築ソフト「WEB MART」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 5 月 15 日	2.6
28	「iLunascape for Android」における WebView クラスに関する脆弱性	Android アプリケーション「iLunascape for Android」には、WebView クラスに関する問題がありました。このため、第三者により当該製品のデータ領域にある情報が窃取される可能性がありました。	2012 年 5 月 21 日	2.6
29	「魔法少女まどか☆マギカ iP for Android」における情報漏えいの脆弱性	Android アプリケーション「魔法少女まどか☆マギカ iP for Android」には、ユーザの入力した Twitter のアカウント情報を平文でログファイルに出力してしまう問題がありました。このため、第三者により Twitter のアカウント情報を取得されるが窃取される可能性がありました。	2012 年 6 月 1 日	2.6
30	「Flash Player」における同一生成元ポリシー実装不備の脆弱性	動画再生ソフト「Flash Player」には、同一生成元ポリシー実装不備の脆弱性がありました。このため、第三者により再生中の音声波形データを、同一生成元ポリシーに反して取得される可能性がありました。	2012 年 6 月 11 日	2.6
31	「Dolphin Browser」における WebView クラスに関する脆弱性	Android アプリケーション「Dolphin Browser HD」および「Dolphin for Pad」には、WebView クラスに関する問題がありました。このため、第三者により当該製品のデータ領域にある情報が窃取される可能性がありました。	2012 年 6 月 14 日	2.6
32	「WEB PATIO」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「WEB PATIO」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 19 日	2.6

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
33 (*1)	「Python SimpleHTTPServer」におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバ「Python SimpleHTTPServer」には、クロスサイト・スクリプティングの脆弱性がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2012 年 6 月 19 日	2.6

（*1）：オープンソースソフトウェア製品の脆弱性
（*2）：製品開発者自身から届けられた自社製品の脆弱性
（*3）：組込みソフトウェアの脆弱性

（2）海外 CSIRT 等と連携して公表した脆弱性

表 1-4、表 1-5 は JPCERT/CC が海外 CSIRT 等と連携し、今四半期に公表した脆弱性および対応状況を示しています。今四半期に公表した脆弱性は 36 件あり、うち表 1-4 には通常の脆弱性情報 30 件、表 1-5 には対応に緊急を要する Technical Cyber Security Alert の 6 件を示しています。これらの情報は、通常関連する登録済み製品開発者へ通知したうえ、JVN に掲載しています。

表 1-4.米国CERT/CC (*6) 等と連携した脆弱性関連情報および対応状況

項番	脆弱性	対応状況
1	TP-Link 8840T の初期設定に問題	注意喚起として掲載
2	Netgear FVS318N の初期設定に問題	注意喚起として掲載
3	Intuit QuickBooks に複数の脆弱性	注意喚起として掲載
4	Java for Mac OS における複数の脆弱性に対するアップデート	注意喚起として掲載
5	Pluck SiteLife にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
6	Rugged Operating System (ROS) におけるユーザアカウントに関する問題	注意喚起として掲載
7	Oracle データベース TNS リスナーに脆弱性	緊急案件として掲載
8	PHP-CGI の query string の処理に脆弱性	注意喚起として掲載 複数製品開発者へ通知
9	Apple iOS における複数の脆弱性に対するアップデート	注意喚起として掲載
10	Apple Mac OS X における複数の脆弱性に対するアップデート	注意喚起として掲載
11	Apple Safari における複数の脆弱性に対するアップデート	注意喚起として掲載
12	Apple QuickTime における複数の脆弱性に対するアップデート	注意喚起として掲載
13	HP Business Service Management に任意のコードが実行される脆弱性	注意喚起として掲載
14	MobileTrack に複数の脆弱性	注意喚起として掲載
15	Seagate BlackArmor NAS に脆弱性	注意喚起として掲載
16	dotCMS に任意のコードが実行される脆弱性	注意喚起として掲載
17	Bloxx Web Filtering に複数の脆弱性	注意喚起として掲載
18	AutoFORM PDM に複数の脆弱性	注意喚起として掲載
19	ISC BIND にサービス運用妨害 (DoS) の脆弱性	緊急案件として掲載
20	Quagga にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載 複数製品開発者へ通知

(*6) CERT/Coordination Center：1988 年のウイルス感染事件を契機に米国カーネギーメロン大学に設置された CSIRT。

項番	脆弱性	対応状況
21	Symantec Endpoint Protection Manager にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
22	複数のビデオドライバが ASLR 機能をサポートしていない問題	注意喚起として掲載
23	ScrumWorks Pro に権限昇格の脆弱性	注意喚起として掲載
24	ForeScout CounterACT にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
25	Apple iTunes における複数の脆弱性に対するアップデート	注意喚起として掲載
26	BMC Identity Management Suite にクロスサイトリクエストフォージェリの脆弱性	注意喚起として掲載
27	Intel CPU で動作する 64bit OS や仮想化環境に権限昇格の脆弱性	注意喚起として掲載
28	Bradford Network Sentry に複数の脆弱性	注意喚起として掲載
29	Java for Mac OS における複数の脆弱性に対するアップデート	注意喚起として掲載
30	Simple Certificate Enrollment Protocol (SCEP) の実装に問題	注意喚起として掲載

表 1-5.米国US-CERT [*7] と連携した脆弱性関連情報および対応状況

項番	脆弱性
1	Adobe 製品における複数の脆弱性
2	Microsoft 製品における複数の脆弱性に対するアップデート
3	Microsoft 製品における複数の脆弱性に対するアップデート
4	Microsoft Windows における証明書に関する問題
5	Microsoft 製品における複数の脆弱性に対するアップデート
6	Microsoft XML コアサービスに脆弱性

[*7] United States Computer Emergency Readiness Team：米国の政府系 CSIRT。

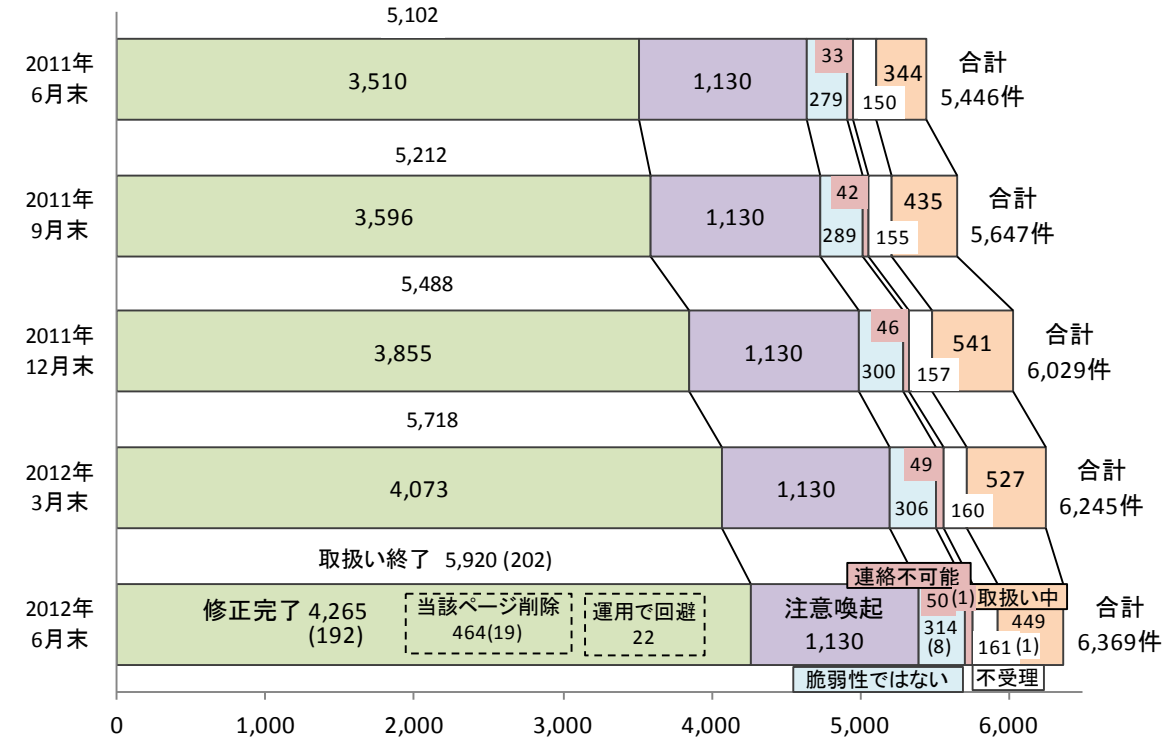
2. ウェブサイトの脆弱性の処理状況の詳細

2.1 ウェブサイトの脆弱性の処理状況

図 2-1 はウェブサイトの脆弱性関連情報の届出における、処理状況の推移を示したものです。ウェブサイトの脆弱性について、今四半期中に処理を終了したものは 202 件（累計 5,920 件）でした。このうち「修正完了」したものは 192 件（累計 4,265 件）、ウェブサイトが利用しているソフトウェア製品の修正プログラムが適用されていない問題について、IPA による「注意喚起」で広く対策実施を促した後に処理を取りやめたものは 0 件（累計 1,130 件）、IPA およびウェブサイト運営者が「脆弱性ではない」と判断したものは 8 件（累計 314 件）でした。なお、メールでウェブサイト運営者と連絡が取れない場合は電話や郵送手段で連絡を試みるなどの対応をしていますが、それでもウェブサイト運営者と連絡が取れず「連絡不可能」なものは 1 件（累計 50 件）です。「不受理」としたものは 1 件（累計 161 件）でした。

取扱いを終了した累計 5,920 件のうち「注意喚起」「連絡不可能」「不受理」を除く累計 4,579 件（77%）は、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されたことを確認しました。

「修正完了」したもののうち、ウェブサイト運営者が当該ページを削除することにより対応したものは 19 件（累計 464 件）、ウェブサイト運営者が運用により被害を回避しているものは 0 件（累計 22 件）でした。



①修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
該当ページを削除	：	修正完了のうち、当該ページを削除して対応したもの
運用で回避	：	修正完了のうち、運用により被害を回避しているもの
②注意喚起	：	IPA による注意喚起で広く対策実施を促した後、処理を取りやめたもの
③脆弱性ではない	：	IPA およびウェブサイト運営者が脆弱性はないと判断したもの
④連絡不可能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの
⑤不受理	：	告示で定める届出の対象に該当しないもの
⑥取扱い中	：	ウェブサイト運営者が調査、対応中のもの

図 2-1.ウェブサイト各時点における脆弱性関連情報の届出の処理状況

2.2 ウェブサイトの運営主体の種類

図 2-2 のグラフは過去 2 年間に IPA に届出のあったウェブサイトの脆弱性関連情報のうち、不受理とした届出を除いたウェブサイトの運営主体の種類別届出件数の四半期別推移を示しています。今四半期も企業が多く届出されています。

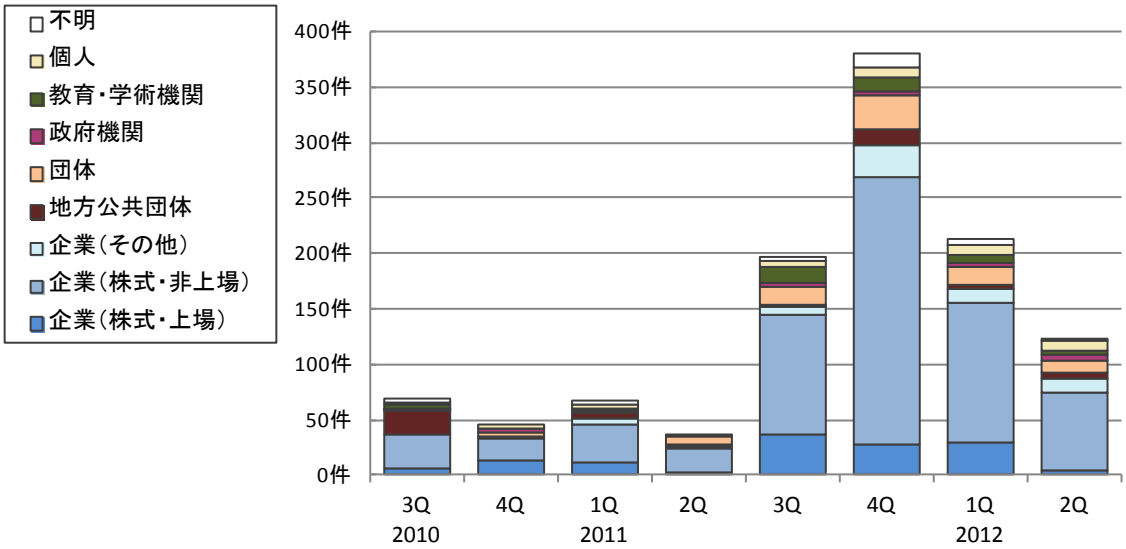
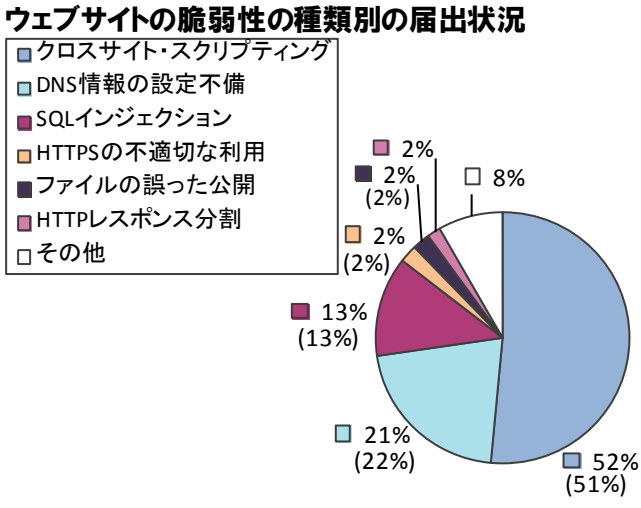


図2-2. ウェブサイトの運営主体の種類別の届出件数（四半期別推移）

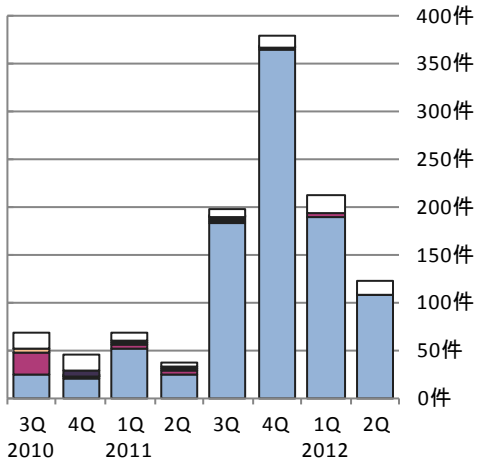
2.3 ウェブサイトの脆弱性の種類と脅威

届出受付開始から今四半期までにIPAに届出のあったウェブサイトの脆弱性関連情報 6,369 件のうち、不受理とした届出を除いた 6,208 件について、図 2-3 のグラフは脆弱性の種類別の届出件数の割合を、図 2-4 は過去 2 年間の脆弱性の種類別届出件数の四半期別推移をそれぞれ示したものです[*8]。脆弱性の種類は届出の多い「クロスサイト・スクリプティング」「DNS情報の設定不備」「SQLインジェクション」の 3 種類の脆弱性が全体の 86%を占めています。2008 年第 3 四半期から 2009 年第 3 四半期にかけて多く届出のあった「DNS情報の設定不備」は、2009 年第 4 四半期以降は届出がありません。今四半期の届出（123 件）のうち、「クロスサイト・スクリプティング」だけで 87%（107 件）を占めます。



（6,208件の内訳、グラフの括弧内は前四半期までの数字）

図2-3. 脆弱性の種類別の届出件数の割合

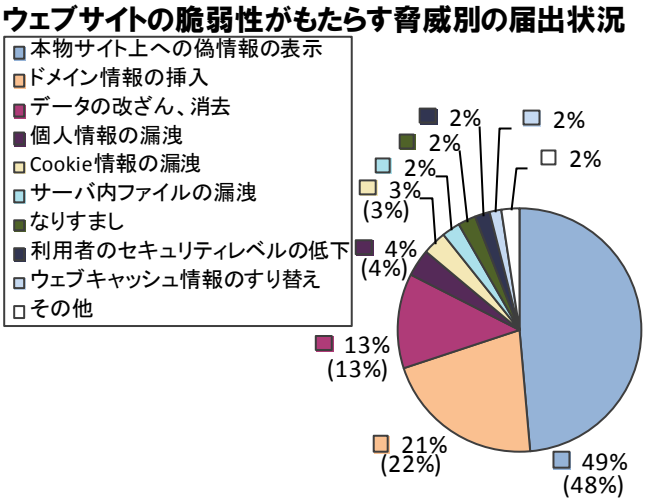


（過去2年間の届出内訳）

図2-4. 脆弱性の種類別の届出件数（四半期別推移）

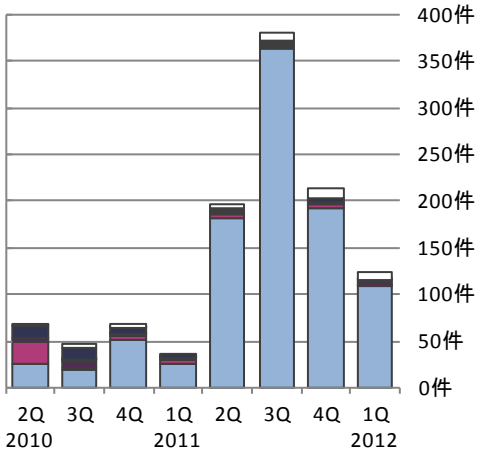
[*8] それぞれの脆弱性の詳しい説明については付表 2 を参照してください。

届出受付開始から今四半期までに IPA に届出のあったウェブサイトの脆弱性関連情報 6,369 件のうち、不受理とした届出を除いた 6,208 件について、図 2-5 のグラフは脅威別の届出件数の割合を、図 2-6 は過去 2 年間の脅威別届出件数の四半期別推移をそれぞれ示したものです。「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 83%を占めています。



(6,208件の内訳、グラフの括弧内は前四半期までの数字)

図2-5. 脆弱性がもたらす脅威別の届出件数の割合



(過去2年間の届出内訳)

図2-6. 脆弱性がもたらす脅威別の届出件数 (四半期別推移)

2.4 ウェブサイトの脆弱性の修正完了状況

図 2-7 のグラフは、ウェブサイトの脆弱性について過去 3 年間の四半期別の修正完了件数を示しています。表 2-1 は、過去 3 年間の四半期末の時点で、修正が完了した全届出のうち、ウェブサイト運営者に脆弱性関連情報を通知してから、90 日以内に修正が完了した件数の割合を示したものです。今四半期は、前四半期と比較して「90 日以内」に修正が完了した割合が低下し、「91 日以上」に修正が完了した割合が上昇しています。

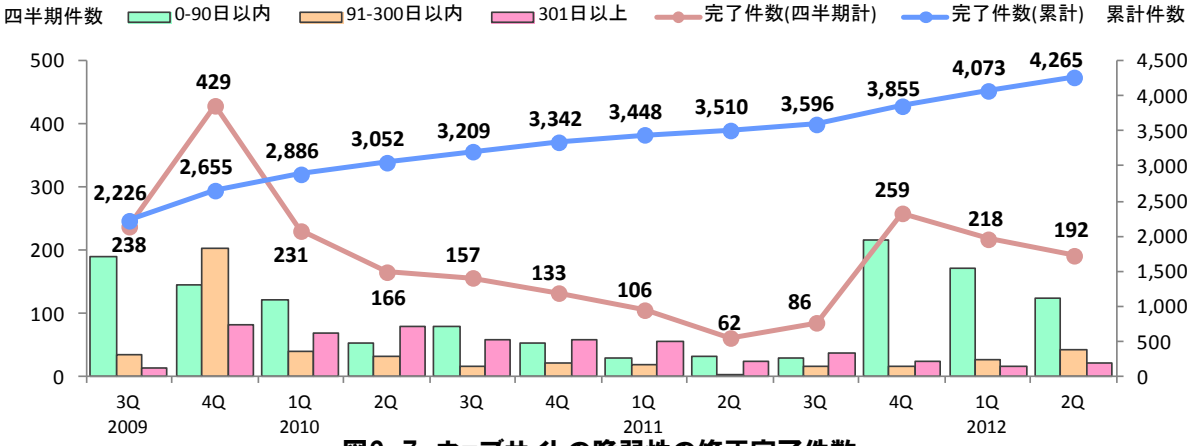


図2-7. ウェブサイトの脆弱性の修正完了件数

表 2-1. 90 日以内に修正完了した件数および割合の推移

	2009 3Q	4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q
修正完了件数	2,226	2,655	2,886	3,052	3,209	3,342	3,448	3,510	3,596	3,855	4,073	4,265
90 日以内の件数	1,760	1,905	2,028	2,082	2,163	2,216	2,247	2,280	2,311	2,528	2,700	2,825
90 日以内の割合	79%	72%	70%	68%	67%	66%	65%	65%	64%	66%	66%	66%

図 2-8 および図 2-9 は、ウェブサイト運営者に脆弱性関連情報を通知してから修正されるまでに要した日数およびその傾向を脆弱性の種類別に示したものです[(*9)]。全体の 47%の届出が 30 日以内、全体の 66%の届出が 90 日以内に修正されています。

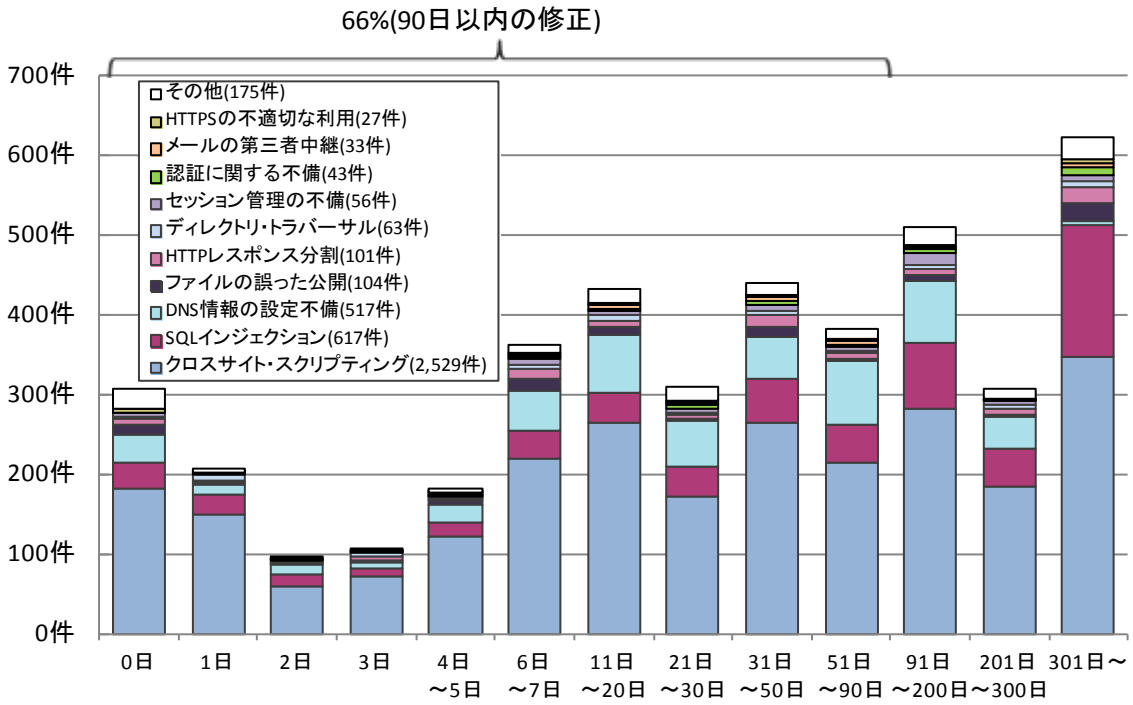


図2-8.ウェブサイトの修正に要した日数

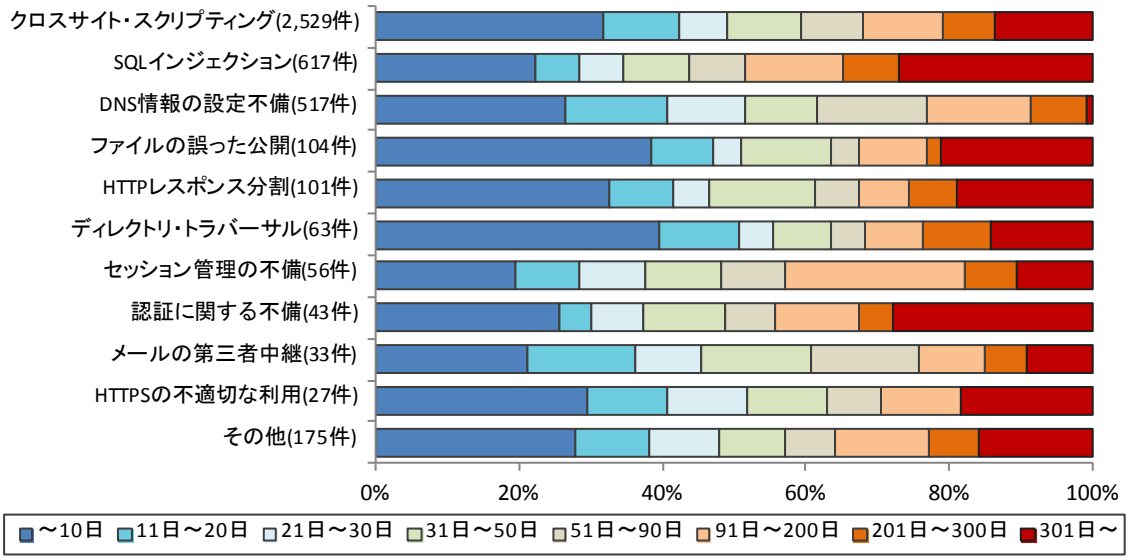


図2-9.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

(*9) 運営者から修正完了の報告があったもの、および、脆弱性が修正されたと IPA で判断したものも含めて示しています。なお、0 日は詳細情報を通知した当日に修正されたもの、または運営者へ詳細情報を通知する前に修正されたものです。

2.5 ウェブサイトの脆弱性の取扱中の状況

ウェブサイト運営者から脆弱性を修正した旨の通知が無い場合、IPA は脆弱性が攻撃された場合の危険性を分かりやすく解説することや、1～2 か月毎に電子メールや電話、郵送などの手段で脆弱性対策の実施を促しています。

図 2-10 は、ウェブサイトの脆弱性関連情報のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性関連情報を通知してから、90 日以上脆弱性を修正した旨の報告が無い）しているものについて、経過日数別の件数を示したものです。経過日数が 90 日から 199 日に達したものは 89 件、200 日から 299 日のものは 66 件など、これらの合計は 318 件（前四半期は 298 件）です。前四半期末までの取扱い長期化 298 件のうち今四半期に 53 件が取扱い終了となった一方、新たに 73 件が 90 日以上経過し取扱い長期化に加わり、合計で前四半期から取扱い長期化の件数が 20 件増加しました。

表 2-2 は、過去 2 年間の四半期末時点で取扱い中の届出について、取扱いが長期化している届出件数および、長期化している割合の四半期別推移を示しています。今四半期は経過日数が 90 日から 199 日に達したものは前四半期と同様に多く、200 日から 299 日に達したものが前四半期の約 7 倍に増加しています。これは、2011 年第 3 四半期以降の届出が、修正されずに長期化したためです。

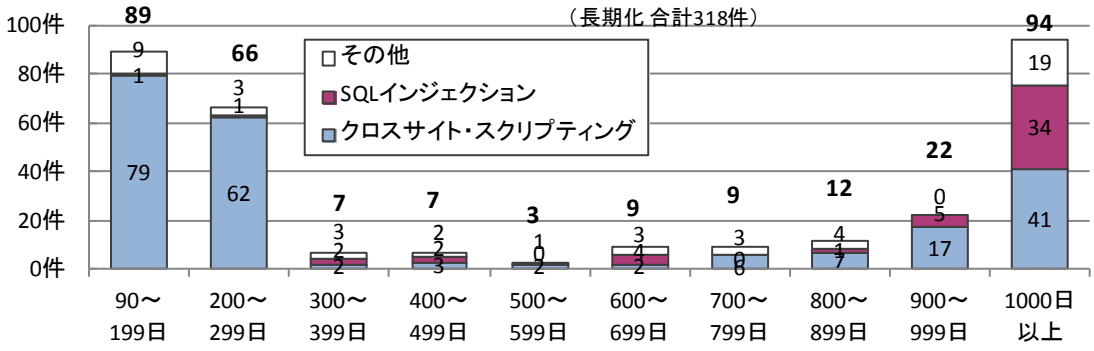


図2-10.取扱いが長期化（90日以上経過）しているウェブサイトの経過日数と脆弱性の種類

表 2-2. 取扱いが長期化している届出件数および割合の四半期別推移

	2010 3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q
取扱い中件数	536 件	436 件	388 件	344 件	435 件	541 件	527 件	449 件
長期化している件数	394 件	359 件	309 件	289 件	228 件	237 件	298 件	318 件
長期化している割合	74%	82%	80%	84%	53%	44%	57%	71%

ウェブサイトの情報が盗まれてしまう可能性のある SQL インジェクションのように、**深刻度の高い脆弱性でも修正が長期化しているものがあります。ウェブサイト運営者は脆弱性を攻撃された場合の脅威を認識し、迅速な対策を講じる必要があります。**

3. 関係者への要望

脆弱性の修正促進のための、各関係者への要望は以下のとおりです。

（1）ウェブサイト運営者

多くのウェブサイトで利用しているソフトウェアに脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェアを利用しているかを把握し、脆弱性対策を実施することが必要です。

なお、脆弱性の理解にあたっては、以下のコンテンツが利用できます。

「知っていますか？脆弱性（ぜいじゃくせい）」: http://www.ipa.go.jp/security/vuln/vuln_contents/

「安全なウェブサイト運営入門」: http://www.ipa.go.jp/security/vuln/7incidents/

また、対策実施にあたっては、以下のコンテンツが利用できます。

「安全なウェブサイトの作り方」: http://www.ipa.go.jp/security/vuln/websecurity.html

「安全な SQL の呼び出し方」: http://www.ipa.go.jp/security/vuln/websecurity.html

「Web Application Firewall 読本」: http://www.ipa.go.jp/security/vuln/waf.html

（2）製品開発者

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報について、「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整を進められるよう、「製品開発者リスト」へ登録ください（URL：https://www.jpcert.or.jp/vh/regist.html）。また、製品開発者自身が自社製品に関する脆弱性関連情報を発見した場合も、対策情報を利用者へ周知するために JVN を活用できます。JPCERT/CC もしくは IPA へ連絡してください。

なお、製品開発にあたっては、以下のコンテンツが利用できます。

「TCP/IP に係る既知の脆弱性検証ツール」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

「TCP/IP に係る既知の脆弱性に関する調査報告書」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」:
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

「ファジング活用の手引き」、「ファジング実践資料」:
http://www.ipa.go.jp/security/vuln/fuzzing.html

（3）一般インターネットユーザー

JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がける必要があります。脆弱性があるソフトウェアを使い続けることは避けなければなりません。

なお、MyJVN（URL：http://jvndb.jvn.jp/apis/myjvn/）では以下のツールを提供しています。

「MyJVN 情報収集ツール」: http://jvndb.jvn.jp/apis/myjvn/mjcheck.html
脆弱性対策情報を効率的に収集するためのツール。

「MyJVN バージョンチェッカ」: http://jvndb.jvn.jp/apis/myjvn/vccheck.html
利用者の PC、サーバ上にインストールされたソフトウェア製品のバージョンを容易にチェックする等の機能。

（4）発見者

脆弱性関連情報の適切な流通のため、届出した脆弱性関連情報は、脆弱性が修正されるまでの期間は第三者に漏れぬよう、適切に管理してください。

付表 1. ソフトウェア製品 脆弱性の原因分類

	脆弱性の原因	説明	届出において 想定された脅威
1	アクセス制御の不備	アクセス制御を行うべき個所において、アクセス制御が欠如している	設定情報の漏洩 通信の不正中継 なりすまし 任意のスクリプトの実行 認証情報の漏洩
2	ウェブアプリケーションの脆弱性	ウェブアプリケーションに対し、入力された情報の内容の解釈や認証情報の取扱い、出力時の処理に問題がある。「クロスサイト・スクリプティング」攻撃や「SQL インジェクション」攻撃などに利用されてしまう	アクセス制限の回避 価格等の改ざん サービス不能 資源の枯渇 重要情報の漏洩 情報の漏洩 セッション・ハイジャック 通信の不正中継 なりすまし 任意のコマンドの実行 任意のスクリプトの実行 任意のファイルへのアクセス 認証情報の漏洩
3	仕様上の不備	RFC 等の公開された規格に準拠して、設計、実装した結果、問題が生じるもの	サービス不能 資源の枯渇
4	証明書の検証に関する不備	ウェブブラウザやメールクライアントソフトに証明書を検証する機能が実装されていない、または、検証が正しく行われずに、偽の証明書を受けいれてしまう	証明書の確認不能 なりすまし
5	セキュリティコンテキストの適用の不備	本来、厳しい制限のあるセキュリティコンテキストで取り扱うべき処理を、緩い制限のセキュリティコンテキストで処理してしまう	アプリケーションの異常終了 情報の漏洩 任意のコードの実行 任意のスクリプトの実行
6	バッファのチェックの不備	想定外の長さの入力が行われた場合に、長さをチェックせずバッファに入力してしまう。「バッファオーバーフロー」攻撃に利用されてしまう	サービス不能 任意のコードの実行 任意のコマンドの実行
7	ファイルのパス名、内容のチェックの不備	処理の際のパラメータとして指定されているディレクトリ名やファイル名、ファイルの内容をチェックしていない。任意のディレクトリのファイルを指定できてしまい、「ディレクトリ・トラバーサル」攻撃に利用されてしまう。また、破損したファイルや不正に書き換えられたファイルを処理した際に不具合が生じる	アプリケーションの異常終了 サービス不能 資源の枯渇 任意のファイルへのアクセス 認証情報の漏洩

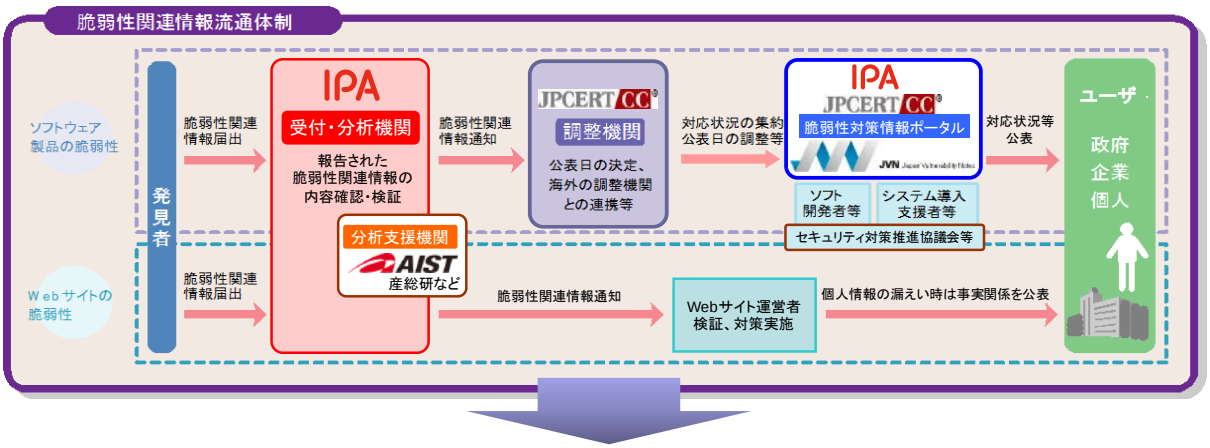
付表 2. ウェブサイト脆弱性の分類

	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
3	ディレクトリ･トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリにアクセスできる	個人情報の漏洩 サーバ内ファイルの漏洩
4	セッション管理の不備	高	セッション管理に、推測可能な情報を使用しているため、他のユーザの情報が容易に推測でき、他のユーザになりすまして、サービスを利用することができる	Cookie 情報の漏洩 個人情報の漏洩 なりすまし
5	SQL インジェクション	高	入力フォームなどへ SQL コマンド（データベースへの命令）を入力し、データベース内の情報の閲覧、更新、削除などができる	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去
6	DNS 情報の設定不備	高	DNS サーバに不適切な情報が登録されているため、第三者がそのドメイン名の持ち主であるかのようにふるまえてしまう	ドメイン情報の挿入
7	オープンプロキシ	中	外部の第三者により、他のサーバへのアクセスを中継するサーバとして利用され、不正アクセスなどの際にアクセス元を隠すための踏み台にされてしまう	踏み台
8	クロスサイト･スクリプティング	中	ユーザの Cookie 情報を知らないうちに転送させたり、偽の情報を表示させたりするような罠のリンクをユーザにクリックさせ、個人情報等を盗むことができる	Cookie 情報の漏洩 サーバ内ファイルの漏洩 個人情報の漏洩 データの改ざん、消去 なりすまし 本物サイト上への偽情報の表示
9	クロスサイト・リクエスト・フォージェリ	中	ユーザを罠のページに誘導することで、そのユーザが登録済みのサイトにひそかにアクセスさせ、登録情報の変更や商品の購入をさせることができる	データの改ざん、消去
10	HTTP レスポンス分割	中	攻撃者がユーザに対し、悪意のある要求をウェブサーバに送信するように仕向けることで、ウェブサーバからの応答を分割させて応答内容をすり替え、ユーザに対して偽のページを表示させることができる	ウェブキャッシュ情報のすり替え
11	セキュリティ設定の不適切な変更	中	ユーザに対し、ソフトウェアをインストールさせたり、ブラウザのセキュリティレベルを下げるよう指示することでクライアント PC のセキュリティ設定を低下させる	利用者のセキュリティレベルの低下
12	リダイレクタの不適切な利用	中	ウェブサーバに設置したリダイレクタが悪意あるリンクへの踏み台にされたり、そのウェブサイト上で別のサイト上のページを表示させられてしまう	踏み台 本物サイト上への偽情報の表示

	脆弱性の種類	深刻度	説明	届出において想定された脅威
13	フィルタリングの回避	中	ウェブサイトのサービスやブラウザの機能として提供されているフィルタリング機能が回避される問題。これにより、本来制限されるはずのウェブページを閲覧してしまう	利用者のセキュリティレベルの低下 なりすまし
14	OS コマンド・インジェクション	中	攻撃者がウェブアプリケーションを介してウェブサーバの OS コマンドを実行できてしまい、サーバ内ファイルの閲覧やシステム操作、不正なプログラムの実行などを行われてしまう	任意のコマンドの実行
15	メールの第三者中継	低	利用者が入力した内容を管理者が指定したメールアドレスに送信する機能で、外部の利用者が宛先メールアドレスを自由に指定できてしまい、迷惑メール送信の踏み台に悪用される	メールシステムの不正利用
16	HTTPS の不適切な利用	低	HTTPS による暗号化をしているが、暗号の選択や設定が十分でなかったり、ウェブサイトでのユーザへの説明に間違いがある、または、ウェブサイトの設計上、ユーザから証明書が確認できない	なりすまし
17	価格等の改ざん	低	ショッピングサイトにおいて、価格情報等が利用者側で書き換えられる。書き換えによる被害は、ウェブサイト側に限定される	データの改ざん

- API : Application Program Interface
- CGI : Common Gateway Interface
- DNS : Domain Name System
- HTTP : Hypertext Transfer Protocol
- HTTPS : Hypertext Transfer Protocol Security
- ISAKMP : Internet Security Association Key Management Protocol
- MIME : Multipurpose Internet Mail Extension
- RFC : Request For Comments
- SQL : Structured Query Language
- SSI : Server Side Include
- SSL : Secure Socket Layer
- TCP : Transmission Control Protocol
- URI : Uniform Resource Identifier
- URL : Uniform Resource Locator

付図１．「情報セキュリティ早期警戒パートナーシップ」（脆弱性関連情報取扱いの枠組み）



【期待効果】

①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
③個人情報等需要情報の流出や重要システムの停止を予防

※IPA：独立行政法人 情報処理推進機構、JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：独立行政法人 産業技術総合研究所